NETWORKING - CLIENT/SERVER CHAPTER 15

(FILE NAME ON DISK # 2 = S2C15.WPD)

A technology revolution has been taking place in the computer industry in recent years and it is expected to continue well into the future. It concerns the use of the PC, its power, its speed, and connecting that power into networks. The use of networked systems brings about a new set of concepts needed to understand network operations and controls to reduce its vulnerability.

To view a system only as its components can blur its process of operation. The following definitions may help to understand that process.

A **computer communication system** is a system composed of data communication links and nodes that create a tool for the exchange of information among the attached components. This includes hardware and software that may be an integral part of the computer system, a separate entity, such as a communication service or any combination of user-supplied components.

A **data communication network** is a system of communication links consisting of modems, multiplexors, concentrators, front-end processors, data matrix switches, monitoring and control/management equipment, and various leased and switched terrestrial and satellite transmission facilities. They are organized and into a network using standard hardware interfaces, software protocols, and specialized network control applications packages to transmit information from one source to another. It is designed to meet a set of specific goals and requirements over a specified life cycle.

A **network architecture** comprises the functions performed by the network and the interfaces structure, and protocols used to perform them.

System components are connected to one another to form a network. The functioning of the network's architecture must be studied because it is the backbone of a network examination. The user should consider that:

- The examination should limit the scope of the process by eliminating application software from the review. An application software review can best be evaluated in the comprehensive or special examination.

- The cable (or whatever the medium of transmission) is a conduit to the functionality of the process.

- The workstation, computer, modem, printer, router, and bridge must be considered for the functionality of the components in the process of moving bits and bytes through the input to output processes.

- To examine a network it must be understood. There are many ways to portray a network. Few network drawings exist that truly represent the network's functionality.

The basic concepts of a network design are:

- *Layering* – The idea of a network is based on the concept of hierarchical layering. The communication mechanism is built one layer upon another, each one adding functions and capabilities.

- *Peer Layer Protocols* – Communication and synchronization between the distributed parts of a layer.

- *Multiplexing* – The sharing of messages among physical channels, seeking, and selecting a path for a message.

- *Topological Considerations* – Particular characteristics of specialized topologies; e.g., STAR, RING, and BUS.

NETWORK ARCHITECTURE/COMPONENTS

A network is a series of points connected by type of communication channel. The points (nodes) typically include a computer, switching equipment, printers, FAX machines, modems, and other devices.

Topology can be thought of as the shape or the way that the various individual parts of the network are connected for example:

Star Configuration

In a star configuration, all of the workstations are connected to one central system server. In this configuration the central process server controls all of the actions of the network nodes, and communication is processed through the central server. (Figure 15.1)

Ring Configuration

In a ring configuration, each workstation performs some of the services of a server device, and a workstation creates an action to be processed by the system. That action is passed (down the wire) to the next workstation until it reaches the appropriate workstation. (Figure 15.2)

Bus Configuration

In a bus configuration, all of the workstations are connected in a string-like configuration. The difference between the bus and the ring is that a ring has no terminal end whereas the bus has a defined beginning and end. A terminator is usually installed at both ends of the bus. (Figure 15.3)

LOGICAL MODELS

Logical models are conceptual representations of communication links and cables, transmission and switching equipment, and software which allow computers to communicate with each other.

ISO Open System Interconnection (ISO OSI) Model

In an effort to standardize the structure for interconnected computer systems and exchanging information, the Open System Interconnection Model was developed. This model is a foundation for coordinating computer interconnection "standards." The model is a layered hierarchical structure of communicating peer-to-peer protocols. The model defines the functions of each of the "standard" layers, the interfaces between layers, and the protocols used for peer communications. The model is based on the concept of communicating workstations. Components of the layers are described as follows (Figure 15.4):

- *Layer 7 – Application* – User-level and application-specific services and procedures. Distributed applications, information manipulation, resource management, virtual file management, etc.

Figure 15.1
Star Configuration

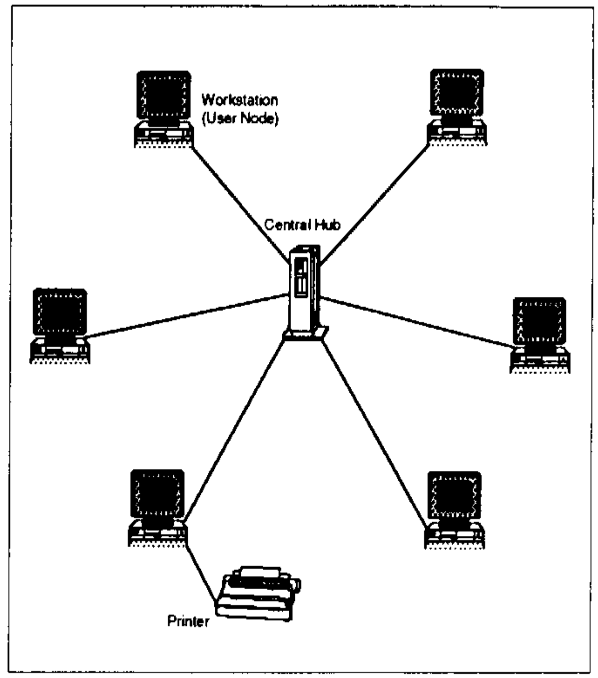


Figure 15.2
Ring Configuration

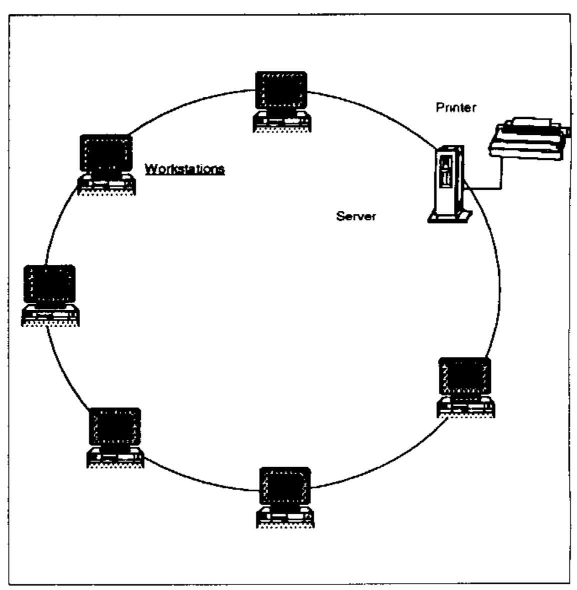


Figure 15.3
Bus Configuration

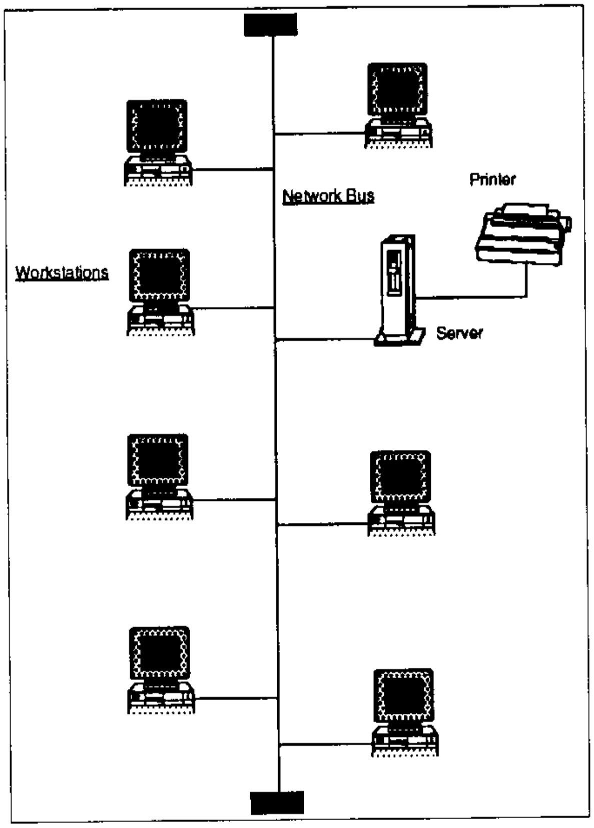
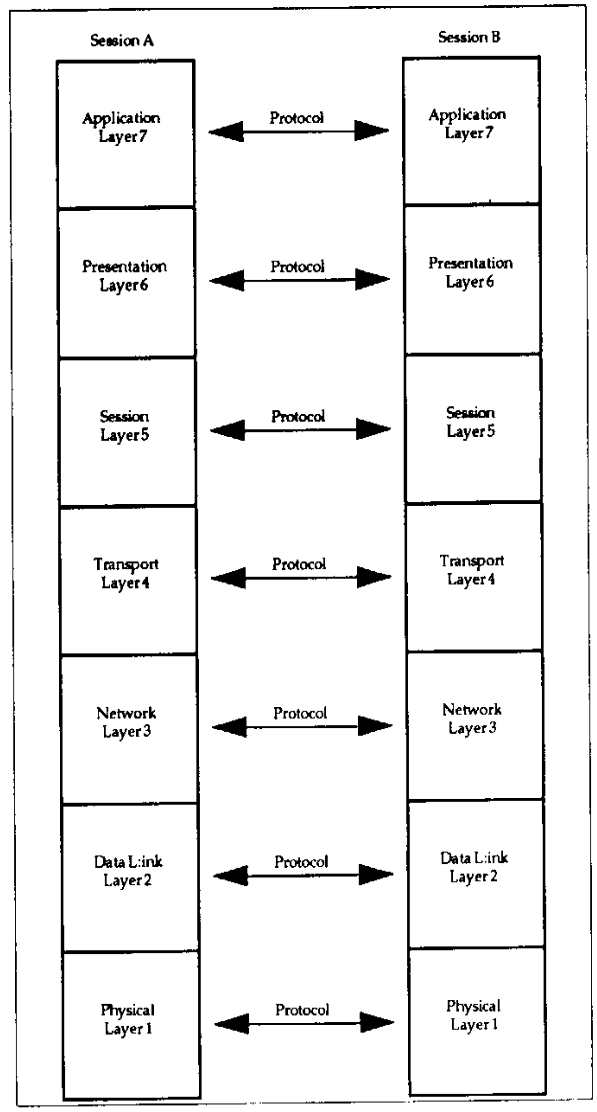


Figure 15.4
ISO Logical Model Open System Interconnection



- *Layer 6 – Presentation* – Representation of information, formats, codes, transformation, encryption, etc.

- *Layer 5 – Session Management* – Conversation initiation, initial screening, access security checking; synchronization, and abnormal recovery.

- *Layer 4 – Transport* – Sending messages. End-to-end control through (possibly multiple) networks. Packet assembly/disassembly (PAD); virtual circuit management, multiplexing, sequencing, message error checking, flow control.

- *Layer 3 – Network* – Sending packets or streams. Network management; routing switching, congestion control; initiating and end-to-end pathway.

- *Layer 2 – Data Link* – Sending blocks/frames. Link management; framing into transmission blocks; synchronization, bit error detection/ correction.

- *Layer 1 – Physical* – Sending bits. Functional and procedural interface to the medium; activate, maintain, deactivate the physical connection; modem control, etc.

- *Layer 0 – Physical Medium* – The medium that carries the energy that carries the information. Electrical/optical/mechanical specifications are considered part of the medium.

Layers 1-3 form the transport or network service. Layer 4 serves as the liaison between the end system and network. Layers 5-7 reflect the end-user system.

IBM SNA – System Network Architecture

The IBM SNA model was introduced in 1974 by IBM. IBM had to migrate existing telecommunications users to SNA, which was evolutionary not revolutionary. This was done to make the network transparent to the users so they would not see the topology, route selection and media and to mask peculiarities of end-users virtual devices. The network was tailored to the specific needs of the users via selectable services. The SNA network provides a communication capability between logical representations of devices and applications.

The OSI model compliments the SNA architecture and each can supplement the other to provide a balanced solution for the management of networks and for the transfer of information between them.

The Consultative Committee on International Telegraph and Telephone's (CCITT) *X.nn* and *V.nn* standards recommend how particular electrical connections should be carried out.

- *X.nn Series Standards* – These are concerned with the connection of digital equipment to public data networks that employ digital signaling.

  X.25 is a standard that describes the interface between terminals operating in the packet mode on public data networks. It is known popularly as the X.25 gateway.

- *V.nn Series Standards* – These are concerned with the connection of digital equipment to a public telephone system that uses analog signaling. There are a number of V.nn standards that relate to public telephone system networks, each with its own set of standard guidelines.

- **LU6.2:** A new part of IBM's SNA is an Advanced Program-to-Program Communication (APPC). APPC is referred to by its two components, logical unit 6.2 (LU6.2) and physical unit 2.1 (PU2.1). IBM describes APPC as a program interface and an operating system. LU6.2 provides a set of conversion verbs that programmers can embed in a program when it needs to communicate with another application, such as to access a database.

OTHER PROTOCOLS AND STANDARDS

Transmission Control Protocol/Internet Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) is the oldest networking standard that was originally developed for military communications. It has been made widely available, especially by its incorporation into the Berkeley Standard Distribution (BSD) release of UNIX. Today, it is implemented on operating systems and available from different vendors. Since each vendor implements its TCP/IP code differently, functionality will vary among vendors.

Synchronous Data Link Control

Synchronous Data Link Control (SDLC) is similar to the X.25. The SDLC protocol begins and ends each frame with a special bit pattern, known as a beginning and ending flag. The beginning flag references the position of the address and control frame elements and initiates error-checking procedures. The ending flag terminates the error-checking procedures.

Token ring networks are used in technical and office environments. Their principle of operation is that whenever a workstation wishes to send a frame, it first waits for a token. On receipt of the token, it initiates the transmission of the frame, which includes the address of the intended recipient. The frame is repeated (that is, each bit is received and retransmitted) by all workstations in the ring, until it circulates back to the initiating workstation, where it is removed. In addition to repeating the frame, the intended recipient retains a copy of it and indicates that this was done by setting the response bits at the end of the frame.

Carrier Sense Multiple Access Collision Detection

The Carrier Sense Multiple Access Collision Detection (CSMA) Ethernet protocol eliminates the collision of messages interfering with each other. If a collision is detected during transmission, the message is held back until some random time interval after the colliding message disappears. Although this does not eliminate collisions completely, it makes them manageable.

DATA TRANSMISSION

The PC as a workstation in a network must have a means of transmission. As data leaves the workstation and begins traveling through the network, it requires a consistent method of transmission over the communication circuits/channels. Binary data can be sent over communication circuits in either parallel or serial modes by use of asynchronous, synchronous, or isochronous transmission methodologies.

Serial Mode

Serial is the primary mode of transferring information in data communications. Serial transmission implies that a stream of data is sent over a communication circuit in a bit-by-bit method. (Figure 15.5)

Figure 15.5
Serial Mode Transfer Circuit

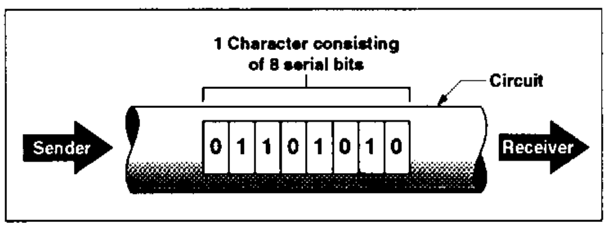
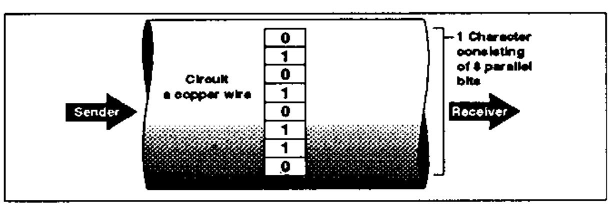


Figure 15.6
Parallel Mode Transfer Circuit



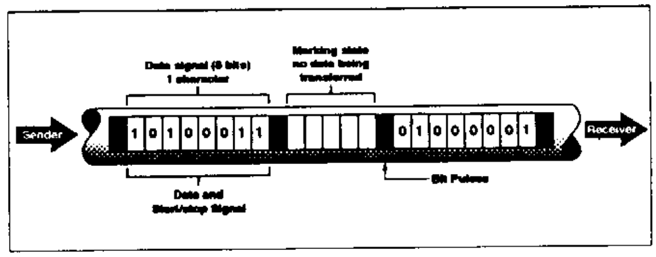
Parallel Mode

Transfers binary data as an *n-bit* all within the same cycle. In other words, if the internal structure of the computer uses an 8-bit element, all eight bits are transferred between the main memory and any operational register within the same computer cycle. More powerful computers use 32 bits. (Figure 15.6)

Asynchronous transmission

For asynchronous transmission, each character must have both a start bit and a stop bit.

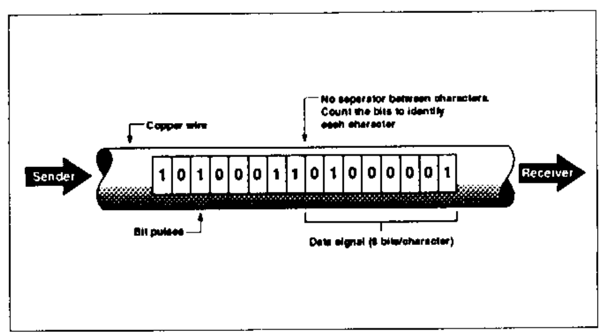
Figure 15.7
Asynchronous Transmission Circuit



Synchronous Data Transmission

For synchronous data transmission, the transmitter and receiver are synchronized. The synchronization time interval between successive bits is specified to an even multiple of the length of one code bit.

Figure 15.8
Synchronous Data Transmission Circuit



Special Devices

- *Modem* – Acronym for modulator/demodulator. It is a device that allows digital data (such as binary output data) to be transmitted, received, and understood over an analog circuit (e.g., voice telephone circuit).

- *Channel service unit (CSU)* – Allows digital data to be transmitted over a digital circuit.

- *Multiplexer* – A device that allows two or more users to share a common physical transmission medium.

- *Encryption* – A ciphering device modifies a signal to make it undecipherable while the signal is on the circuit of the network. A deciphering device is needed at the termination end of the circuit network to make the signal understandable (decryption).

HOST COMPUTER COMPONENTS

Network Operating Systems

The Network Operating Systems (NOS) is the functional heart of the network. Users generally think of the network as central operating software that defines its logical layout and oversees the allocation of its hardware, software, and peripheral resources. The NOS reaches into the physical network as its protocol. Although NOS is far removed from the physical topology of the network, an important relationship exists between it and the underling topology.

From a strategic perspective, it is the services offered by a particular NOS – the applications with which it is comparable, its tools for interconnection and connectivity, its management and its administrative resources – that often comprise the key factors in designing a LAN. The NOS has a direct affect on the topology chosen for the network.

UNIX

UNIX is an operating system that facilitates telecommunications and networks, but its acceptance has been slow in the commercial sectors. In 1988 AT&T and Sun Microsystems made a major investment and effort to make UNIX a foundation system. While it had the necessary functionality for communications, UNIX has not been widely used in business because of its lack of user-friendliness, business application, operating system facilities (security, file management), and on-line transaction processing. Those problems are being resolved, and UNIX may be increasingly accepted as a mainstream commercial operating system for business applications. UNIX has become one of the most widely used operating systems today. It provides multitasking, multiuser, heterogenous, computing environment on hardware platforms ranging from mainframes to PCS.

The primary feature of UNIX is its ability to provide application portability. Portability allows free movement of applications between dissimilar operating systems without having to recreate application interfaces. UNIX advantages include the ability to: support multitasking and multiuser environments; support multiple DOS sessions; allow mapping of UNIX and DOS disks to one another; allow DOS applications to act as clients to the UNIX-based file server; provide a platform for distributed systems computers in client/server

Telecommunications Access Method

Telecommunications Access Method (TCAM) replaces and extends both BTAM and QTAM (BTAM, or Basic Telecommunications Access Method, provides the basic functions to control data communication circuits. QTAM, or Queued Telecommunications Access Method, is an extension of BTAM that includes all of the BTAM facilities but will not support synchronous communications. See Chapter 31: Glossary for additional information). TCAM resides in the host computer. The most significant features are those used for network control and system recovery.

Virtual Telecommunications Access Method

Virtual Telecommunications Access Method (VTAM) is data communication software that complements IBM's advanced hardware and software. It resides in the host computer. VTAM manages a network structure based on SNA principles. It directs the transmission of data between application programs in the host computer and the components of the data communications network.

EXTERNAL CONNECTIONS

Gateway

A gateway connects two dissimilar networks, including two different communication architectures, and operates at layer seven of the OSI model. Gateways are associated with LANs and translate one network protocol into another, convert data formats, and open sessions between application programs.

Bridge

A bridge is designed to increase the number of addressable nodes on a network or to link two geographically distant, but similar, networks that use the same protocol. When two network segments are bridged, all traffic on either segment will pass on the other segment.

Routers

Routers join two networks that may be similar. The network segments joined by the router do not necessarily need to be of the same type: a router can connect an Ethernet to a Token Ring and to a public X.25 data network.

A router distinguishes data packets according to their protocol type and forwards traffic according to the logical or protocol address (rather than the hardware addresses that are used by a bridge).

Repeaters

Repeaters are simple devices that pass all traffic in both directions between the LAN segments they link. Repeaters are not discriminating. They are hardware devices that relay all they receive. A repeater extends the distance over which a network can be operated.

COMMUNICATIONS MEDIA AND CARRIERS

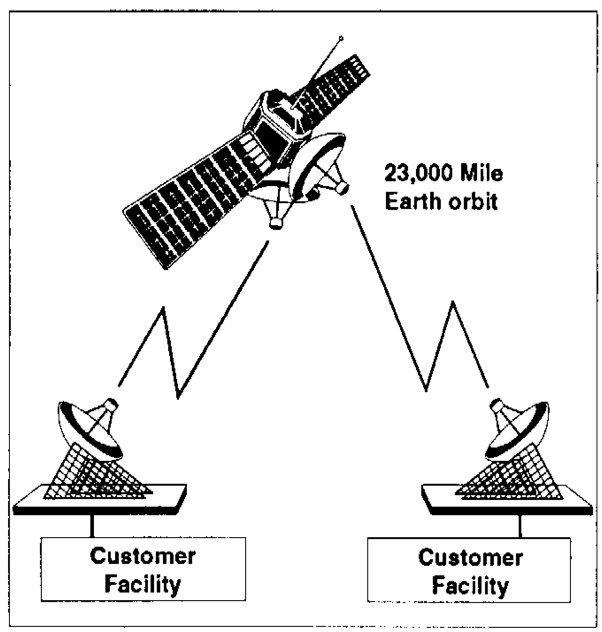
All communicated messages are carried by a type of medium. Communications carriers may be as common as a voice telephone system, or more specialized than public mailbox services and may be located on the LAN. The media may be arranged so that different network configurations and the components can be provided by specialized carriers.

- **Copper wire** is the most common metallic conductor for transmitting signals; it is used by telephone companies. Cabling connections with copper wire are made using standard jacks. Twisted wire pair is a form of copper wires used in the transmission circuits. Paired cable can be a few wires or several thousand twisted pairs.

- **Coaxial cable** is copper and sometimes aluminum wires bundled together to provide band-width transmissions of analog or digital signals. Insulated coaxial cable can be buried, run under water, or laid throughout a building on walls, ceilings, and floors.
- **Fiber optics** cable is composed of micro-thin fibers, usually glass, that use light energy rather than electrical energy. Information is transmitted as pulses of highly focused light. Fiber optic cable can carry a broad bandwidth with low signal degradation in less space than copper or coaxial cable. Fiber optic cable is more difficult to tap than copper or coaxial cable. Fiber optics cable also is immune to environmental conditions.

- **Satellite** communication begins at an earth station, passes through a satellite in geosynchronous orbit above the earth, and ends at one or more earth stations. The satellite serves as an active relay, and its communications relay systems, consisting of transponders and antennas, are its most important components. (Figure 15.9)

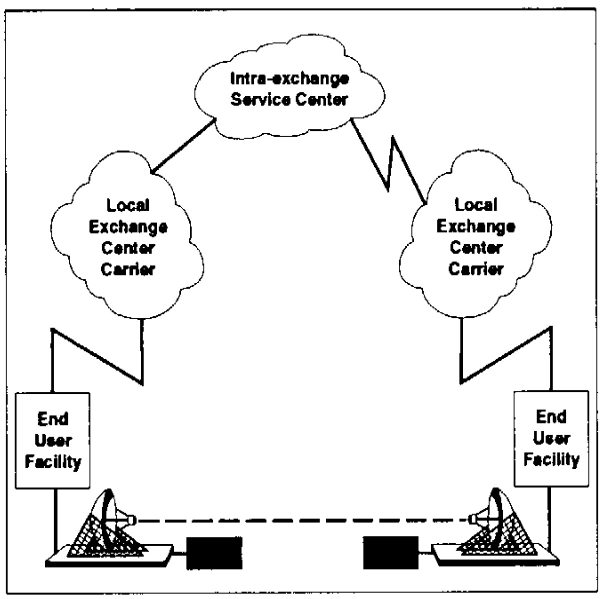
Figure 15.9
Satellite Services Configuration



These systems receive end-user transmissions from sending earth stations, amplify them, and retransmit them to receiving earth stations. The signal at the transmitter is much stronger than the one at the receiver. Since simultaneous signals at the same frequency interfere with one another, the satellite converts the signal it receives to another frequency before transmission.

- **Microwave** communication describes point-to-point radio. Microwave communications was once the domain of common carriers, but it has become a major competitor of standard, wire-line telephone communications. Microwave communications involves sending waves of information between a radio transmitter and a radio receiver, each generally mounted on a tower. It requires a clear line-of-sight. There can be no obstructions in the path of the transmitting and receiving antennas. (Figure 15.10)

Figure 15.10
Microwave Communications



NETWORK CONFIGURATIONS

Local Area Network

A local area network (LAN) is a data communication system that connects intelligent computer devices and peripherals and software, so that they can communicate and share resources, such as storage devices, programs, and data files. It integrates a wide range of functions into a single system. LANs are generally fault tolerant, incorporating a simple architecture with control distributed among participating stations. Since the entire network does not depend on a single polling or switching device, the failure of one component does not bring down the entire LAN.

Metropolitan Area Network

Metropolitan area networks (MANs) generally include several locations within a single metropolitan area.

Wide Area Network

When computers are located in different cities, public-carrier facilities must be used again. This network is known as a wide area network (WAN). The type of WAN used will depend on the nature of the application. This means that a WAN can span the globe.

The use of high-capacity communication lines, coupled with standard transmission protocols, over long distances provides the capability to tie geographically diverse processors or multiple vendors into a single environment. The processors on this network can be accessed equally by any user, providing that appropriate communications software is available to the user on either a microcomputer that emulates a network-attached terminal or on a mainframe that the user is able to access.

Value Added Network

Value added networks (VANs) are constructed with leased lines (circuits) and serve many customers in different geographical areas. Usually they are general purpose computer networks similar to the ones developed by public companies, such as Telenet, Tymnet, US Sprint, and MCI. These VAN carriers transmit either data or voice. A VAN is designed to allow a large number of users to use the network for a fee, usually based on the time spent on the network or the volume of data transmitted.

The VAN is a good alternative when volume or traffic requirements are low, or when an organization is not prepared to maintain and manage a private network, or when special services, such as mailboxes are required. The VAN adds the risk of the service provider to that of the using organization.

Client/Server

Client/server computing is an application of cooperative processing in which a programmable workstation executes a portion of the application.

This type of computing allows an application to be divided into logical components that can be distributed among several connected devices.

Client/server is characterized generally by the division of an application into components processed on different networked computers. The client/server is made up of two distinguishable entities: a client, which requests a service or information from a server; and a server, which processes the request, performs the service, and returns the requested information to the client. The client/server model has the following capabilities:

- The client and the server can interact seamlessly.
- The client and the server are located on separate platforms and are connected by the network.
- The server can serve multiple clients concurrently and, conversely, a client can access multiple servers.
- The client or the server can be upgraded individually.

Applications, based on the client/server model of computing, provide a great latitude in deploying application functionality across the network. This flexibility enables the use of desktop and portable devices, which, when working with high-power, low-cost servers, helps provide a cost-effective business solution. The client/server supports customers making the transition from transaction-based processes to business-event and knowledge-based solution. This transition is accomplished by new technology enablers, such as graphical user interfaces (GUIs), multimedia, and imaging, on an enterprise level.

Standards are a crucial element in client/server architectures, defining the interface between clients and servers and ensuring client application portability, interoperability, and maintainability.

The immature nature of client/server architectures is a concern of the client/server system. Organizations are often forced to choose among proprietary approaches that may not be the most effective approach for the institution.

The following fundamental attributes are associated with the client/server architecture:

- A many-to-many relationship exists between clients and servers. One server can support multiple clients at the same time, and one client can access multiple servers at the same time.
- A server in turn becomes a client to another server. A server can change roles depending on whether it provides resources to a client or requests resources from another server.
- Clients and servers can be, and usually are, replicated throughout the network.
- Requests for servers are initiated by clients. Servers cannot initiate requests to clients.

Peer-to-Peer Network

This type of network gives every microcomputer access to all nodes of the network's resources. In a network of peers, any microcomputer can share its hard disk and printer with any other microcomputer. The network's users create names for their local printers and disk volumes and designate them as sharable network resources. Unlike server-based networks, peer-to-peer networks allow shared resources attached to any microcomputer without going through an intermediary, such as a central microcomputer server.

MANAGEMENT OF NETWORKS

As networks become larger and more complicated, tools must be provided for their management. Originally, such tools were needed only for managing WANs, since the long-haul lines were quite expensive and problems needed to be detected and fixed immediately, usually from a central location.

Today, the network system is an integral part of most organizations' communications infrastructure. Problems affect many or all users quickly and visibly. These changes have increased the scope of network management to cover the management of applications, so that the total effort is called systems management. There is little difference in control concepts necessary to manage systems and networks.

Network management requires mechanisms to define and monitor control information. Some systems, such as Novell's NetWare Management System (NMS), allow the area network administrator to manage the NetWare LANs and attached devices that are spread throughout the enterprise-wide network. The basic functions of NMS include network fault detection, performance, configuration, security, and accounting management.

Change Management

Change management is a process to control changes in the system so that changes are properly developed, tested, documented, and approved. The concept is similar to the mainframe process, wherein a user requests a change to the network configuration, access level, and authorization. All changes should be well documented and follow standard change management procedures.

Ideally, two environments should exist in the system, a test and a production environment. Software should be tested off line. A test and acceptance plan should be developed and executed. The movement of the test system to production should be carried out using procedures and controls similar to mainframe software production change controls.

Failure Diagnosis

Analyzers are generally considered test sets that allow operators to simulate specific message streams to test devices, communication circuits, or other workstations. Analyzers fall into several categories, which include a protocol analyzer, response time analyzer, and data line monitor. Generally, however, these tools perform the same basic tasks.

An analyzer measures the responses of all hardware in the network. This equipment can determine whether the network meets its performance specifications. These devices detect the content (bits) of a frame or packet during its transmission. For example, it might measure poll-to-poll time, which is the time from the detection of the poll being sent to the terminal, until the time that the poll is again sent to the same terminal. Another could be the measurement of poll or response time. A protocol analyzer also can trap information when certain character sequences appear on the send or receive communication network. Performance response time and link utilization can be captured by some analyzers. Protocol analyzers, response time analyzers, and data line monitors tend to look like a portable microcomputer with a few extra switches and buttons on the front panel.

These devices are, active and passive. Active analyzers/monitors can generate data that are interactive on the circuit and can emulate various terminals because they are programmable. Passive analyzers/monitors merely monitor and collect data to be examined later.

A typical analyzer can monitor data, trap and count data for gathering communication circuit statistics, offer a video screen and printer, poll various stations, offer various protocols, possess breakout box capabilities, etc. It is possible to turn a microcomputer into a combined protocol analyzer, response time analyzer, data line monitor, and Bit-Error Rate Tester (BERT). It requires a PC adapter board, software, and external RS232 interface that can tap into the data line.

Response Time

Most telecommunications network users perceive that the quality of a network's service has a direct relationship to application response time. Poor response time is perceived to be poor quality performance. In reality, application response time is attributable to several factors independent of the network. The network plays a critical role in response time in a poorly designed network, and unnecessarily degrades the response time of its applications. In addition to overloading the network, other sources of poor network response time are line quality, equipment failures, and incorrect software initialization options.

Operations Management

Network availability is vital in an environment where on-line transaction processing applications are critical to the organization. Operational management controls help ensure that the network adequately supports critical applications. Operations management is the day-to-day management of the network. Reactive operations management responds to critical problems. Some general functions of operations management are:

- Making the network available to all users.

- Monitoring network status.
- Reacting to network alerts and alarms.
- Taking immediate, corrective actions to reroute traffic or move to backup equipment in order to increase network user availability.
- Responding to risks of network viruses and other network attacks by implementing appropriate software controls and a viable recovery plan.

Administration

Within a network environment, the network administrator serves many functions. A network administrator would:

- Monitor network efficiency statistics.
- Ensure that all files considered essential are periodically backed up and stored off-site.
- Establish and maintain adequate virus protection facilities on the network.
- Maintain a set of current security tables off-site.
- Reviewing network activity reports.
- Ensuring a source for certified network components exists.

Network Accounting Systems

Accounting management tracks costs associated with network usage. Network accounting systems can be an automated tool to control costs. This type of accounting can provide the ability to:

- Record outgoing calls by station, extension, or account code (for client or customer chargeback).
- Report usage.
- Control operational decisions, such as routing, duration times, and priority.
- Allocate charges for equipment and overhead.

A network accounting system also can provide users with the ability to:

- Identify misuse and abuse of the services.
- Bill telephone time and expenses.
- Allocate costs by department, etc.
- Select the most efficient and economical long-distance telephone networks.

The use of these accounting records enables management to identify fraudulent network use. There are many evolving control-related techniques available as network security controls. A few examples are:

- Time-of-day logging.
- Unusual requests reporting.
- Repeated efforts, etc. (look for anomalies).
- Encourage internal clocks with telephone call-back features.

COMMERCIAL NETWORK SERVICES

The number and range of products and services, including network technologies and vendor choices, resulted from the deregulation of the telephone industry in 1984. That process created a new set of services and providers. Service and installation problems have become more difficult because of the number of different interfaces available. The emphasis is now on competitive pricing (generally thought of as rate information) and cost control.

Because of deregulation, the local operating companies offer services other than communication circuits. These include office automation equipment, multiplexers, switchboards (PBX), modems, cellular mobile equipment, etc. They may become a major manufacturer as well as a seller/distributor in the near future.

The service area of each of the seven Bell Operating Companies is broken into local access transport areas (LATA). These LATAs can offer their own service, but must offer service to other, suppliers including AT&T, MCI, and US Sprint.

The LATAs have created a point of presence (POP). The POP is usually the end office to which the local loop is connected, so that messages can be sent on the long-distance circuit when it leaves the local LATA. AT&T, MCI, and US Sprint have at least one POP in each LATA.

Public data networks, also called public timesharing networks and remote computing services, are available for virtually any data processing application, business function, or information retrieval service that might be desired. They are generally accessed through a subscription service. An organization may use the PDN to access low volume users and/or particularly remote location users. The PDNs ordinarily use dial-up and low-speed voice-grade lines.

Dial-up (Switched) Networks

Dial-up networks provide services through shared switching and transmission facilities. A switched network design assumes that not all users will use the network at the same time and provides alternate paths to increase the probability of call completion. A switched public network may not be able to handle call volume at peak times and can cause delays.

Leased Line (also called Dedicated or Nonswitched Networks)

These are usually private networks that use leased lines between two or more points to keep the line available. Many organizations encrypt leased lines to prevent data disclosure when the risk warrants the cost and transmission overhead.

T Carrier Circuits

T carrier circuts are leased digital circuits with a transmission capacity of 1,544,000 bits per second that move over two pairs of wires. The T carrier system is the standard for interconnecting digital communications. It is a hierarchy of digital transmission and multiplexing standards, ranging from T-1 to T-4.

- *T-1 Circuit* – Any digital communication system operating at a synchronous data rate of 1,544,000 bits per second. Data can be transmitted over a T-1 circuit at speeds ranging from 56,000 to 1,544,000 bits per second. Digitized voice uses 64,000 bits per second. By digitizing voice signals and multiplexing them with time division multiplexing, T-1 circuits allow for 24 simultaneous voice channels.

- *Fractional T-1* – Offers portions of a 1,544,000-bit-per-second T-1 circuit for a fraction of its full cost. Users who use more transmission speed than voice grade can have digital service.

- *T-2 Circuit* – Can transmit at a rate of 6,312,000 bits per second. Basically, a T-2 circuit is a bundle of four T-1 circuits.

- *T-3 Circuit* – Allows transmission at a rate of 44,376,000 bits-per-second (usually referred to as a 45-megabits-per-second circuit). A T-3 circuit is a bundle of 28 T-1 circuits.

- *T-4 Circuit* – Transmits at a rate of 274,176,000 bits per second. This is equal to the bandwidth of 178 T-1 circuits.

MISCELLANEOUS COMMUNICATIONS

Voice

To control voice calls, most business organizations install call management systems. These systems monitor telephone call traffic, point out peak periods, and track efficiency and other voice telephone communications. A hardware box that performs these functions can be installed to work with private branch exchange (PBX) switchboards. The PBX is a switchboard within which all of the telephone lines of an organization terminate. Usually several circuits from this switchboard go to the telephone company's end office. These circuits are generally referred to as trunk lines when devoted to voice and are called leased circuits, private circuits, or dedicated circuits for data transmissions.

Modern digital PBXs can use digital transmission switching techniques because they use 32-bit microprocessor chips that act as the central controller/central intelligence. A typical digital PBX uses a star architecture so that individual telephones or microcomputers can be connected directly to the central digital switchboard. Modern digital PBXs provide simultaneous transmission of voice and data.

A voice type circuit is an analog transmission. Therefore, digital signals passed over the analog circuit must be converted. This conversion is done by a type of modem.

Communication services are supplied by AT&T, one or more of the seven regional Bell Operating Companies, MCI, US Sprint, General Telephone and Electronics (GTE), or one of the other common carriers.

Private circuit (lease) services are services leased from one of the common carriers. In other words, the private circuits are available for use by an organization 24 hours a day, 7 days a week, and charge a flat rate.

Measured use services are those for which charges are based on usage measured in time. In a Wide Area Telephone Service (WATS), a fixed monthly fee is charged for a number of circuit-hours used. If the time is exceeded, the rate or fee is increased. Some of the primary services in this group are direct dialing, WATS, 800/900 service, and packet switching.

Facsimile

The fax is a device that scans a document, converts it to digital data and transmits the digitized representation over the communication circuit. A like device is used to receive and translate the digitized image for printing. A fax uses a modem to transmit and receive the data. Current fax technology can be incorporated into both the send and receive functionality of a personal computer and/or LAN system.

In contrast to the low bandwidth available with a connection through an analog-switched telephone network, the usable bandwidth of a coaxial cable can be much higher. This potentially high bandwidth can be used in one of two ways. In a baseband single-channel mode, all of the available bandwidth is used to drive a single high bit rate along the transmission path. In a broadband channel mode, the bandwidth is divided to derive a number of lower bandwidth subchannels on one cable.

In the baseband mode, the cable is used exclusively for the transmission of data between two systems, that is point-to-point, while in others the normally high bit rate transmission channel is time-shared by a number of systems, referred to as a multipoint or multidrop configuration.

In the broadband mode, multiple (independent and concurrent) transmission channels are derived from a single distribution cable, using a technique known as frequency-division multiplexing (FDM).

Integrated Services Digital Network

Integrated Services Digital Network (ISDN) is a leased service in which the common carrier offers a communication circuit with two 64,000-bits-per-second transmission channels and one 16,000-bits-per-second signaling channel. This is a high speed digital transmission service which can combine simultaneous voice conversations, data transmissions, and image transmissions can be combined. ISDN generally uses coaxial cable or microwave.

POLICIES AND PROCEDURES

Clearly, policies and procedures have been a main stay requirement in computer operations. With networks, they are no less important. Policies and procedures should assure that employees understand:

- The use of assets for management control.
- Procurement processes.
- Hardware and software operational controls.
- Protection and confidentiality of information.
- System development life cycle, change management, security, problem/incident reporting, and contingency planning.

NETWORK SECURITY

This section will, to a limited degree, provide a brief discussion of network security. For a more detailed reference on general security, refer to the Information Systems Security section in this handbook.

Network management must control the security of the network and the data stored and transmitted over it. The security is intended to prevent data loss and unauthorized access.

Physical Security

Management should prevent the unauthorized user from physical access to network devices or the transmission media.

Logical Access Security

Logical access security controls are designed to prevent users from gaining unauthorized access to the network resources or applications.

Many networks now use satellite, microwave, or other transmission modes to exchange data and information. One method to safeguard the information transmitted is to encrypt the data.

User identification (ID) and passwords are common in computer networks. Although IDs and passwords are considered a good practice, controls and change procedures are necessary to guard against their vulnerability more effectively.

Passwords are the first line of defense against a breach to a network's security. Several restrictions can be placed on passwords to improve their effectiveness.

Minimum Password Length and Format. If a user is allowed to change the password, rules should govern the minimum character length of the selected password. There should be rules that prevent the use of easily guessed passwords (a simple rule may include forbidding common words and/or requiring that special characters be used as part of the password).

- *Forced Periodic Password Change*. Forcing periodic changes to passwords is an important component of password security. However, frequency of change also has a down-side in that users have difficulty remembering new passwords.

User time and location controls when employed properly will enhance security. The controls demand, transmission or session usage be limited to specific devices and specified times.

Switched ports are among the most vulnerable security points on a network. These allow dial-in and dial-out access. They are security risks, because they allow users with telephone terminals to access systems. Although call-back is a potential control, it is not necessarily the most effective, because of the call-forwarding capability of telephone circuits.

Transaction logs can be an important aspect of network security. Every login attempt should be logged. The logging control should include the date, time, user ID and password used, the location, and number of unsuccessful attempts made.

Computer viruses are executable computer programs that may propagate, using other programs as carriers. They sometimes modify themselves during or after replication. A virus performs unwanted functions on a computer. Some viruses perform simple annoying functions, while others erase or modify programs or critical data. Viruses are typically introduced into a network by floppy disks, and the network propagates them throughout the system (See Chapter 14 for additional information on information systems security).

DISASTER RECOVERY

The concept of disaster recovery and planning has long been understood in the mainframe computer environment. With the proliferation of networks, disaster recovery planning has become equally important to critical network operations. Like mainframe disaster recovery, networks need:

- Network disaster planning.
- Network backup procedures.

For additional information about disaster recovery (See Chapter 10: Corporate Contingency Planning for additional information).

LEGALLY ENFORCEABLE STANDARDS

Legally enforceable standards provide criminal punishment for three types of computer criminals: those who gain access to federal computers; those who gain unauthorized access to computers at financial institutions that are covered by federal laws; and those who gain access to computers that hold national security data. Many states have additional laws on computer communications security in order to supplement and/or enhance the following federal statutes:

- *Federal Wiretap Stature of 1968* protects voice communications from interception.
- *Electronic Communications Privacy Act of 1986*

makes it a federal crime to intercept electronic communications, such as data communications or electronic mail, or to tamper with computers in a data network. This law also includes the intentional transmission or distribution of unauthorized software that damages computer data, software, or hardware.

- *Computer Fraud and Abuse Act of 1986* expands the jurisdiction of computer crimes to include those involving the private sector computers located in two or more states. The law also addresses the so-called private bulletin board systems that exchange computer passwords.

- *Computer Security Act of 1987* requires federal agencies to create information security standards.

- *Computer Virus Eradication Act of 1988* was created to fight the spread of computer viruses. The law prohibits programs for computers, or a computer itself, or information or commands that may cause loss, expense, or risk to the health or welfare of the user organization. The law also bans giving such programs to others.

RISKS AND CONTROLS

Risks

Application systems are available to network users through the telecommunications architecture. The controls required of the network will depend on the type of applications available on the network and the business the network supports.

Risks include the unauthorized access of confidential data, the unauthorized modification of data, business interruption, and incomplete and inaccurate data. Some examples include:

- The loss of network availability that may have a serious, perhaps a financial impact, on the business or service.

- Obsolescence of the network components, including hardware, software, communications, etc.

- Unauthorized and indiscriminate use of synchronous and asynchronous modems to connect to the network to other networks.

- Connection of the network to public switched telephone networks.

- Inaccurate, unauthorized, and unapproved changes to systems.

- Performance thresholds that do not isolate problems, including system faults, inventories, an audit trail, and historical data record.

- Service degradation and delayed problem solution by vendors, leading to inconsistencies and incompatibilities among components of the network.

Controls

On-line interactive systems require specialized telecommunications controls. Some examples include:

- Physical network security that prevents accessing the network devices or transmission media.

- Logical access security to prevent unauthorized use of the network once physically connected.

- Keeping the telephone numbers of the in-house network confidential, using of tone suppression devices on all ports, limiting network availability using authorization and authentication mechanisms, limiting access by location, and monitoring failed logon attempts.

CLIENT/SERVER INTRODUCTION

Traditional information technology in financial institutions employed a large central computer system. Increasingly, financial institutions are employing client/server (C/S) technology to develop and deliver mission critical products and services. Client/server technology uses a network typically installed in a business unit, rather than a centralized computing facility.

Client/server technology enables business units to develop and deliver products and services to market much quicker than traditional legacy methods. The tradeoff is that controls over these systems are typically substandard to those associated with traditional systems. That is, the use of client/server technology, unless developed with a high level of controls, increases the level of transactional risk in the institution. The reason for the substandard level of controls is that business unit managers are typically not information systems technology professionals. Yet, these managers find themselves with the responsibility for making decisions on employing client/server technology to meet their business requirements. The boards of directors and senior management of financial institutions should be aware of their responsibility to address risks associated with client/server computing and to encourage the development and implementation of sound policies, practices, or procedures and controls over client/server computing environments.

C/S BACKGROUND

The traditional approach to data processing for banking functions has been to develop and use large mainframe or midrange systems which are expensive to acquire and maintain. These systems require special physical environments and lengthy application development processes. Application developers have not always kept up with development requests that would allow financial institutions to provide faster delivery of services and products. End users, who need immediate solutions, have become frustrated with this traditional approach to data processing. This new technology is now available, at a perceived cost savings, that could satisfy end user demand for more timely management information system solutions.

End user needs have led to increasing acquisitions of computers and commercial off-the-shelf programs by departments, business units, and individuals to reduce their dependence on a centralized data processing environment. However, this strategy has its own limits. For example, stand-alone computers make it difficult to share information with other information systems. This problem is being solved by the development of high-speed data transmission and network file servers in client/server computing.

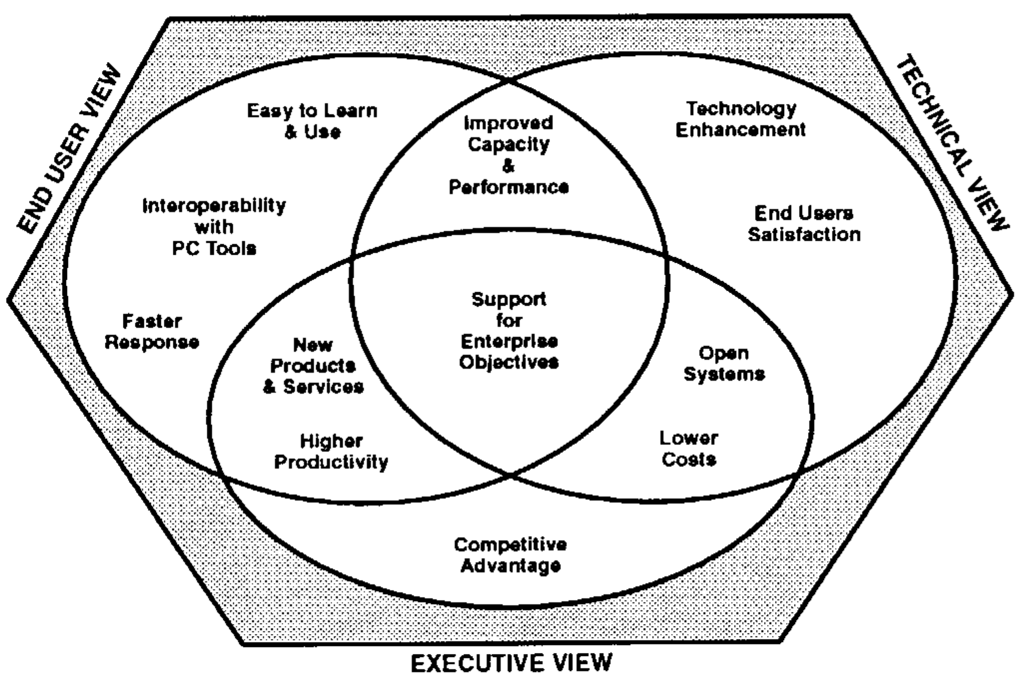
As a result, financial institutions are now processing mission-critical applications including funds transfer, branch automation, general ledger reporting, security portfolio accounting, and customer relationship management on client/server systems. Additionally, independent service providers (service bureaus) also are utilizing this new technology by providing these systems as part of their servicing operations to financial institutions. (Figure 15.11)

ROLE OF SENIOR MANAGEMENT

The board of directors of financial institutions must develop and adopt appropriate policies, practices, or procedures covering management's responsibilities and controls for all areas of client/server computing activities. Management must recognize that the implementation of controls is just as important in the client/server environment as in the mainframe environment. The institutions strategic planning should clearly define the technological and control architecture. End users and auditors must have a prominent role in the acquisition, development, and implementation of all client/server computing environments. (Figure 15.12)

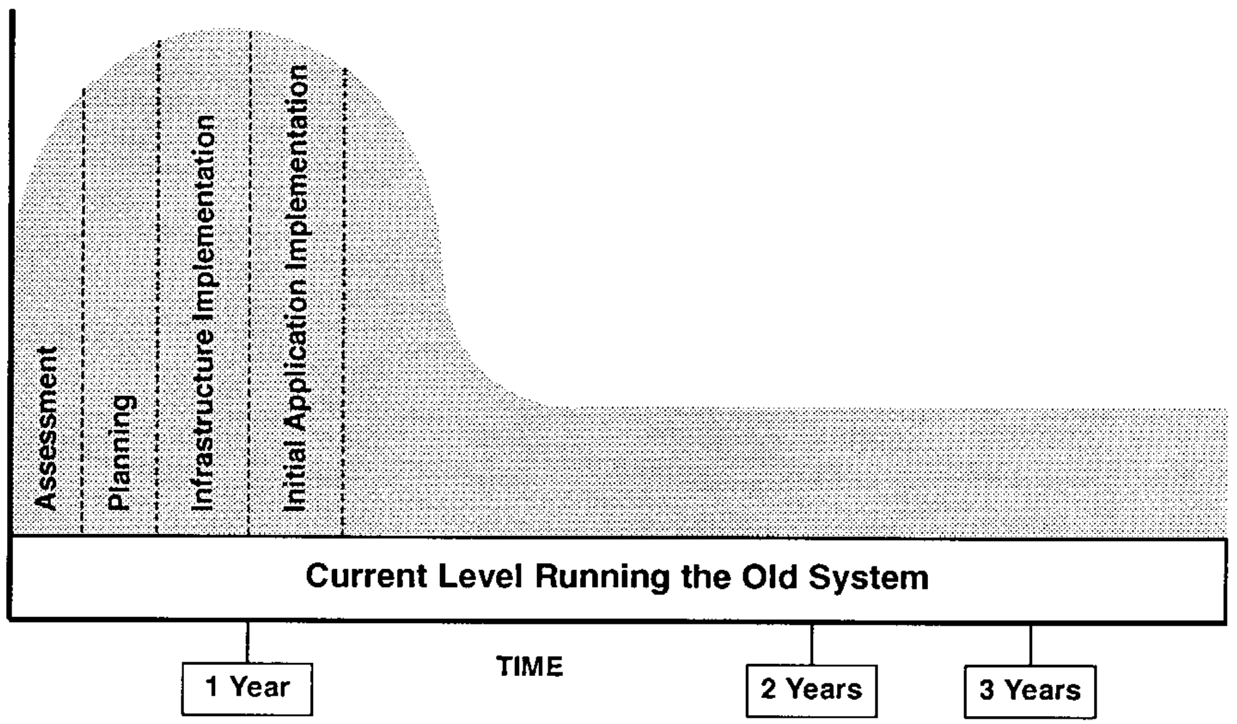
The existence of policies, practices, or procedures and the management supervision of client/server activities will be evaluated by examiners during regular supervisory reviews of the institution. See Chapter 25 and FFIEC SP-3: Joint Interagency Issuance on End-User Computing Risks for additional information.

Figure 15.11
Client/Server Can Be a Cohesive Force in the Enterprise Executive View



With Permission M. Zola Rapid Systems Solutions, Inc.

Figure 15.12
Client/Server Can Be a Cohesive Force in the Enterprise



With Permission M. Zola Rapid Systems Solutions, Inc.

DEFINITIONS

Client/server computing is a method of allocating data processing resources in a network so that computing power is distributed among workstations in the network. This type of computing allows integrated applications (general ledger, demand deposit accounting, loans, etc.) to share system and data resources using cooperative processing. Cooperative processing differs from traditional mainframe or distributed system processing in that each processing component is mutually dependent.

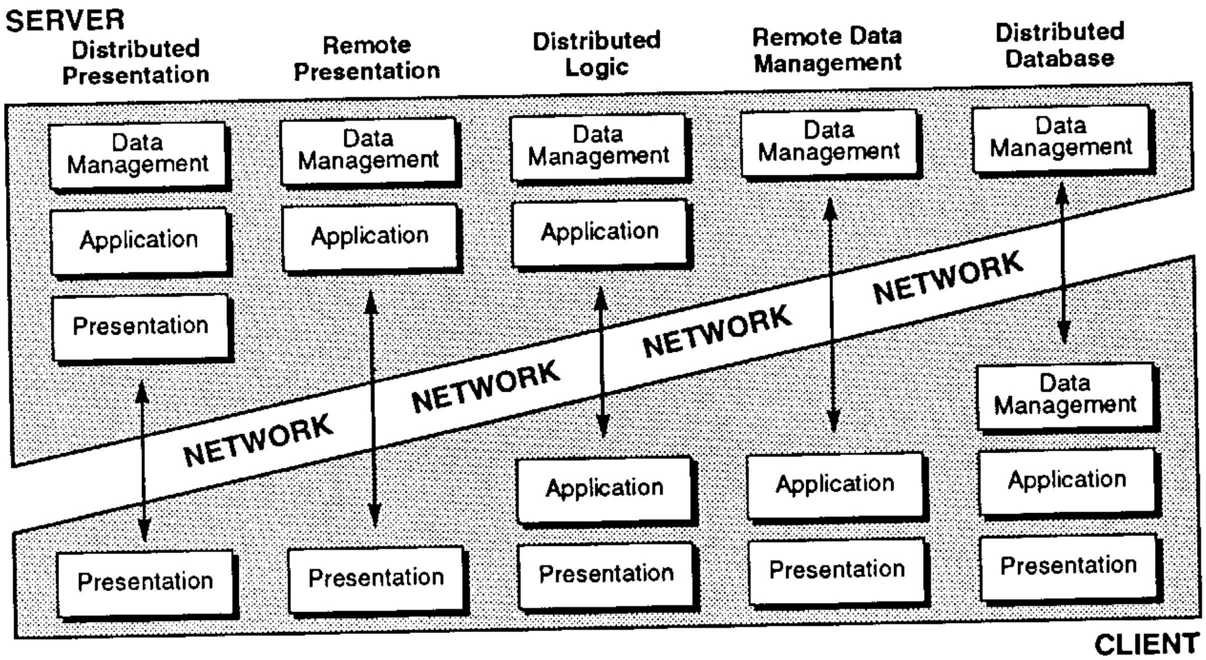
C/S COMPONENTS AND CHARACTERISTICS

- *Client* – A client (front-end) is a single PC or workstation associated with software that provides computer and presentation services as an interface to server computing resources. Presentation is usually provided by visually enhanced processing software known as a Graphical User Interface (GUI).

- *Server* – A server (back-end) is one or more multi-user computer, usually a mainframe or a minicomputer, although it could be a PC. Server functions include any centrally supported role, such as file sharing, printer sharing, database access and management, communication services, facsimile services, application development, and others. Multiple functions may be supported by a single server.

- *Middleware* – This is a client/server specific term used to describe a unique class of software employed by client/server applications. This software resides between an application and the network, and manages the interaction between the GUI front-end and data servers in the back- end. It facilitates the client/server connections over the network and allows client applications to access and update remote databases and mainframe files.

Figure 15.13
Types of Client/Server Computing



With Permission M. Zola Rapid Systems Solutions, Inc.

- *Distributed* – Most commonly, a server is a distinct computer that serves any number of client systems. It is feasible to have clients and servers on the same computer. The server may be in the same room as its clients, or it may be across town or around the world.

- *Decentralized* – Client/server systems are typically installed, administered, and operated by a business unit, rather than a centralized computing facility.

- *Complex* – Client/server systems usually involve multiple clusters of computers linked by high-speed communication lines. (Figure 15.13)

ISSUES AND RECOMMENDATIONS

The proliferation of client/server technology introduces new risks as well as benefits. In today's competitive environment, client/server technology can be a strategic initiative of the organization, and therefore is not just a technological concern, it is also a business concern. Customer demand for flexible and timely management information has fostered its growth. Faster delivery of services, ability to leverage emerging technology, autonomy of end users, and productivity gains from re-engineering the work flow are all potential benefits.

The client/server architecture has not evolved to the point where controls are inherent in the design, maintenance, and operation of the system. Controls are more difficult to implement effectively due to the distributed, decentralized and complex nature of the client/server environment. A prior section of this chapter illustrated some of the risks and controls that have been associated with network computing. These are also applicable to the client/server environment.

The need for controls over information systems environments is not new. What has changed is the control and decision making responsibility. Traditional or legacy systems were controlled centrally. That is, most banks had large central computer resources with corresponding centralized software development resources. One of the reasons banks have migrated to the client/server technology is to reduce the lead time on bringing new products and services to market. This can happen very quickly in a client/server environment where the business unit rather than a central resource has control over the computer and software development resources. Unfortunately, not all business units have the software engineering expertise to develop systems with the high level of controls expected of bank information systems. With this decentralization of decision making over technology, larger banks can have literally thousands of client/server systems without any centralized management oversight or requirements for interoperability or compatibility.

Some of the control issues include logical access controls, i.e. controls which limit access to the banks computer systems and the activities performed once access is granted. Contingency planning is not always a consideration when developing these systems. For a mission critical system, lack of contingency planning could significantly impact the bank. Testing of the systems can be compromised in an effort to gain market presence. Accordingly, the cost of re-engineering can negate the anticipated savings of time and resources associated with a decision to implement client/server technology. Absence of controls over data base access through client/server systems could compromise the data base and the integrity of resulting management information.